基于区块链且支持数据共享的密文策略隐藏访问控制方案

杜瑞忠[1,2]，张添赫[1]，石朋亮[1,2]
（1. 河北大学网络空间安全与计算机学院，河北 保定 071000；
2. 河北省高可信信息系统重点实验室，河北 保定 071000）

摘 要：传统的属性基加密方案虽然实现了一对多的访问控制，但仍存在单点故障、效率低下、不支持数据共享以及隐私泄露等挑战。针对以上问题，提出了一种基于区块链且支持数据共享的密文策略隐藏访问控制方案。利用素数阶双线性群和正负号与门访问结构，实现细粒度访问控制的同时避免了用户属性值的泄露；结合以太坊和星际文件系统解决了用户属性撤销问题和云存储模型中的单点故障问题，通过代理重加密的方法实现了数据共享。基于困难问题假设，证明了所提方案的安全性。仿真实验结果表明，所提方案在实现策略隐藏的同时具有较高的效率。

关键词：属性基加密；策略隐藏；区块链；数据共享；属性撤销
中图分类号：TP309
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.20221119

Ciphertext policy hidden access control scheme based on blockchain and supporting data sharing

DU Ruizhong[1,2], ZHANG Tianhe[1], SHI Pengliang[1,2]
1. School of Cyber Security and Computer, Hebei University, Baoding 071000, China
2. Key Lab on High Trusted Information System in Hebei Province, Baoding 071000, China

Abstract: Although the traditional attribute-based encryption scheme achieves one-to-many access control, there were still challenges such as single point of failure, low efficiency, non-support for data sharing, and privacy leakage. In response to the above problems, a ciphertext policy hidden access control scheme based on blockchain and supporting data sharing was proposed. The prime order bilinear group and the AND-gates on+/− were used to achieve fine-grained access control while avoiding the leakage of user attribute values. Ethereum and interplanetary file system were combined to solve the problem of user attribute revocation and the single point of failure problem in the cloud storage model, and data sharing was realized through proxy re-encryption. Based on the assumption of difficult problems, the safety of the scheme was proved, and the simulation experiment results show that the proposed scheme has high efficiency while implementing policy hiding.

Keywords: attribute-based encryption, policy hidden, blockchain, data sharing, attribute revocation

0 引言

随着物联网技术、云计算、大数据等新兴技术的发展，越来越多的个人和组织用户将其数据进行在线存储及远程共享。用户可以随时随地访问并获取数据。然而，存储在云端的数据可能包含大量的隐私和机密，一旦受到攻击或缺乏监控，可能造成数据被篡改或隐私泄露等重大事故[1]。数据加密被认为是实现数据安全的有效方法之一。

收稿日期：2022−02−28；**修回日期：**2022−05−26
基金项目：国家自然科学基金资助项目（No.61572170）；河北省自然科学基金资助项目（No.F2019201290）
Foundation Items: The National Natural Science Foundation of China (No.61572170), The Natural Science Foundation of Hebei Province (No.F2019201290)

密文策略属性基加密（CP-ABE, ciphertext policy attribute-based encryption）方案[2]可以实现对外包数据细粒度的访问控制，灵活性和实用性更高，受到了业内的广泛关注，但存在访问策略失效的问题，不支持数据共享。为了解决该问题，已有方案提出了属性代理重加密方案，代理服务器可以对更改后的策略进行重加密从而实现数据共享，但效率较低。

在大多数现有的 CP-ABE 方案中，数据拥有者通常会将加密数据上传到云服务器，一旦云服务器发生问题，会导致整个系统瘫痪，此类方案依赖于云服务器[3-4]，存在单点故障问题。为了解决这一问题，研究者提出了基于权能的访问控制（CapBAC, capability-based access control）方案[5]以及基于区块链的访问控制方案。然而，CapBAC 方案在轻量级的设备上实现分布式访问控制时，由于轻量级设备不能保证自己的安全性，攻击者可以通过安全性薄弱的轻量级设备威胁访问控制的安全，因此 CapBAC 方案无法解决在不可信环境下的访问控制问题。在基于区块链的访问控制方案中，由于区块链的透明性，将访问策略直接部署到区块链上可能会泄露用户的属性信息。例如，在一个分布式的访问控制系统中，患者通过交易将其电子病历访问控制策略存储在区块链中。如果访问控制策略规定医生可以访问，尽管攻击者无法读取电子病历，但仍可以读取存储在区块链上的访问控制策略，则攻击者可以推断出患者可能患有疾病。因此，如何防止恶意用户从访问策略中获取隐私信息也是一个至关重要的问题[6]。

当前，现有的策略隐藏 CP-ABE 方案有 2 种形式，即完全隐藏[7]和部分隐藏[8]。前者是指访问策略不会泄露任何属性隐私；后者是指只有访问策略的部分属性值是匿名的，而访问策略本身仍以明文形式存在。完全隐藏虽然在效率上不及部分隐藏，但是其能提供更好的隐私保护。对于隐私敏感的系统来说，访问策略信息的任何泄露都可能严重威胁数据拥有者的隐私。因此，设计一个策略完全隐藏的 CP-ABE 方案，对保护数据拥有者的隐私来说是至关重要的。

为了解决上述问题，本文提出了一种基于区块链的密文策略隐藏方案，实现访问控制和数据共享的同时还保护了策略隐私。

本文主要研究工作如下。

1) 提出了一种高效的属性向量和策略向量生成算法，在此基础上，利用代理重加密技术和属性加密技术，设计了一种策略完全隐藏的 CP-ABE 方案，不但支持细粒度的访问控制而且实现了数据共享。

2) 利用星际文件系统（IPFS, interplanetary file system）存储密文并通过智能合约将密文哈希地址存储在区块链上。实现分布式且值得信赖的访问控制的同时降低了区块链的存储开销。通过撤销合约维护撤销列表的方式实现了撤销功能，避免了用户私钥滥用问题。

3) 基于困难问题证明了所提方案的安全性。通过仿真实验对所提方案的效率进行了分析说明，验证了所提方案的有效性。

1　相关工作

Saini 等[9]基于区块链的智能合约，实现了以患者为中心和医疗记录可访问的目标，将加密数据存储在云服务器上，减小了区块链的存储开销，但是其方案存在可扩展性和性能方面的问题。Zhang 等[10]结合智能合约技术和基于属性的访问控制模型，提出了一个分布式且可靠的访问控制框架。该框架包括一个策略管理合约、一个属性管理合约以及一个用于执行访问控制的访问合约，由于区块链的公开透明性，该方案存在属性泄露的风险。Phuong 等[11]基于正负号与门访问结构提出了一种策略隐藏访问控制方案，该方案利用韦达定理和内积加密实现了完全策略隐藏，但是该方案在密钥生成阶段以及解密阶段需要针对访问结构中的正负号分别进行一次运算，因此效率较低。王悦等[12]在文献[11]的基础上进行了改进，减少了解密算法的运算次数，但是该方案只是对主密钥以及公共参数进行了优化，依然存在效率较低的问题。Gan 等[13]基于素数阶双线性群提出了一种部分策略隐藏方案，在解密之前加入了解密测试算法，一定程度上提高了解密效率，但该方案效率仍然较低。Zhang 等[14]提出了一种支持密钥撤销的部分策略隐藏方案并设计了一种算法来检查用户属性与访问策略是否匹配，然而该算法会增加用户的计算负担，并且其解密算法效率较低，物联网设备的资源消耗较大。Hao 等[15]利用布隆过滤器提出了一种高效的完全策略隐藏方案，但是该方案不能抵御属性猜测攻击。随后，Arkin 等[16]提出了一种敏感属性选择算法，并使用

布隆过滤器来隐藏敏感属性，提高了策略隐藏的效率，但是该方案同样不能抵御属性猜测攻击。Zeng 等[17]提出了一种具有可追溯性的高效部分策略隐藏方案，但由于该方案是基于合数阶双线性群构建的，因此效率并不理想。以上方案虽然实现了策略隐藏，但是依然存在效率低下、访问策略失效等问题。

为了应对访问策略失效的问题，Gao 等[18]将 CP-ABE 与代理重加密技术相结合提出了一种属性代理重加密方案，可以针对更改后的策略进行重加密，解决了访问策略失效的问题。张小红等[19]提出了一种基于区块链的密文存储共享模型，通过智能合约实现了自主化的密钥转换。然而上述 2 个方案在重加密阶段和重解密阶段的双线性配对次数会随属性个数线性增加，因此效率较低。Paul 等[20]提出了一种高效的属性代理重加密方案，该方案可以使用新策略对密文进行重加密，并且在重加密阶段和重解密阶段双线性配对的次数是固定不变的，因此其效率较高。

综上所述，当前的策略隐藏访问控制方案仍存在效率低下、访问策略失效等问题。为此，本文提出了一种基于区块链且支持数据共享的密文策略隐藏访问控制方案，克服了策略不可更改且效率低下的问题。

2 预备知识

2.1 双线性对

$\mathbb{G}_1$、$\mathbb{G}_2$和$\mathbb{G}_T$同为素数阶为 q 的乘法群，其中，$\mathbb{G}_1 \neq \mathbb{G}_2$，$e$为一个线性映射，$e:\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$，满足以下 3 种性质。

1) 双线性。对于任意的 $g \in \mathbb{G}_1$，$h \in \mathbb{G}_2$，$a,b \in \mathbb{Z}_p$，有 $e(g^a,h^b)=e(g,h)^{ab}$。

2) 非退化性。$e(g^a,h^b) \neq 1$。

3) 可计算性。对于任意的 $g \in \mathbb{G}_1$，$h \in \mathbb{G}_2$，$e(g,h)$可有效计算。

2.2 访问结构

集合 $U=\{U_1,U_2,\cdots,U_L\}$ 代表系统中的用户属性，$U_k \in$ {“+”，“−”}；集合 $P=\{P_1,P_2,\cdots,P_L\}$ 代表访问策略，$P_k \in$ {“+”,“−”,“*”}，$k \in \{1,2,\cdots,L\}$；通配符“*”表示“任意”，即“+”和“−”都接受。例如，U={U_1=“CS”,U_2=“CE”,U_3=“Faculty”,U_4=“Student”}，其中“CS”和“CE”分别代表网络安全专业以及通信工程专业。Alice 是网络安全专业的学生，Bob 是通信工程专业的学生，Carol 是网络安全专业和通信工程专业的教师。访问策略 P_1 允许通信工程专业的教师访问而不允许网络安全专业的学生访问。访问策略 P_2 允许网络安全专业的所有教师和学生访问，但不允许通信工程专业的教师和学生访问。上述用户属性和访问策略如表 1 所示。

表 1 用户属性和访问策略

用户属性	描述	用户			访问策略	
		Alice	Bob	carol	P_1	P_2
U_1	CS	+	−	+	−	+
U_2	CE	−	+	+	+	−
U_3	Faculty	+	−	+	−	*
U_4	Student	−	+	+	+	*

2.3 韦达定理

$\boldsymbol{p}=(p_1,p_2,\cdots p_l)$，$\boldsymbol{u}=(u_1,u_2,\cdots u_l)$ 代表 2 个向量，其中，向量 $\boldsymbol{p}$ 包含符号“+”“−”和通配符“*”，向量 $\boldsymbol{u}$ 仅包含“+”“−”2 个符号。位置集合 $I=(i_1,i_2,\cdots i_n) \subseteq \{1,2,\cdots,l\}$ 代表向量 $\boldsymbol{p}$ 中通配符的位置。因此，如果用户属性满足访问策略，则有 $((p_i=u_i) \vee (p_i=*)), i \in [1,l]$，转化成数学形式为

$$\sum_{i=1,i\notin I}^{l} p_i \prod_{k_w \in I}(i-k_w)=\sum_{i=1}^{L} u_i \prod_{k_w \in I}(i-k_w) \tag{1}$$

$$\prod_{k_w \in I}(i-k_w)=\sum_{j=1}^{n} a_j i^j \tag{2}$$

由式(1)可得

$$\sum_{i=1,i\notin I}^{l} p_i \prod_{k_w \in I}(i-k_w)=\sum_{j=0}^{n} a_j \sum_{i=1}^{L} u_i i^j \tag{3}$$

选取随机群元素 B_i，将 p_i 和 u_i 作为指数，则有

$$\prod_{i=1,i\notin I}^{L} B_i^{p_i \prod_{k\in I}(i-k)}=\prod_{j=0}^{n}\left(\prod_{i=1}^{l} B_i^{u_i i^j}\right)^{a_j} \tag{4}$$

根据韦达定理，式(2)中的系数 a_j 可用 k_w 表示，其中，$0 \leqslant j \leqslant n=|I|$。

$$a_{n-j}=(-1)^j \sum_{1\leqslant i_1 \leqslant i_2 <\cdots< i_j \leqslant n} k_{i_1} k_{i_2} \cdots k_{i_j} \tag{5}$$

2.4　非对称决策双线性 Diffie-Hellman 假设

非对称决策双线性 Diffie-Hellman（DBDH, decisional bilinear Diffie-Hellman）定义为 $g\in\mathbb{G}_1$, $h\in\mathbb{G}_2, a,b,c\in\mathbb{Z}_p$，均匀地随机选取 $T\in\mathbb{G}_T$，如果挑战者给予敌手 (g,g^a,g^c,h,h^a,h^b)，敌手将很难区分有效元组 $e(g,h)^{abc}$ 与随机元组 T。

一个概率性多项式时间算法 A 能以优势 ε 求解 DBDH 问题，当且仅当

$$\left|\Pr\left[A\left(g,g^a,g^c,h,h^a,h^b,e(g,h)^{abc}\right)=0\right]-\Pr\left[A(g,g^a,g^c,h,h^a,h^b,T=0\right]\right|\geqslant\varepsilon$$

如果概率多项式在解决 DBDH 问题上的优势可以忽略不计，则 DBDH 假设成立。

3　方案设计

3.1　系统模型

本文系统模型如图 1 所示，该模型包括以下实体：数据拥有者（DO, data owner），数据用户（DU, data user），可信机构（TA, trusted authority），代理服务器（PS, proxy server），区块链（BC, blockchain）和星际文件系统。

DO。负责制定访问策略，并将其个人数据加密上传到 IPFS 上，通过授权合约将密文相关信息存储在区块链上。

DU。负责向 DO 发送访问请求，通过授权合约的验证后，获取密文地址。

TA。负责系统参数的生成并部署撤销合约，其在系统中是完全可信的。

PS。使用 TA 生成的重加密密钥对密文重加密，假设其是半可信的。

BC。包括授权合约和撤销合约，撤销合约维护一个撤销列表，当用户注销时 TA 将其地址放入撤销列表中。当 DU 发送访问请求时，授权合约判断其是否被撤销，如果没有被撤销，则向 DU 发送密文相关信息，否则拒绝访问。

IPFS。分布式系统，存储密文并返回其哈希地址。

在该系统中，访问控制工作流程可分为准备阶段 0a)～0e)和执行阶段 1)～5)。准备阶段主要进行密钥的分发及密文信息的发布。执行阶段主要进行访问请求的判决及数据共享。

准备阶段。首先 DU 进行注册，TA 生成相关参数并部署撤销合约。DO 根据公钥和访问策略对明文 M 进行加密并将密文存储在 IPFS 上，IPFS 返回哈希地址，然后 DO 部署授权合约并通过交易将密文相关信息存储在区块链上。

执行阶段。在访问控制阶段，DU 向 DO 发送访问请求，授权合约在验证 DU 的身份后将密文相关信息发送给 DU，DU 验证并解密密文。在数据共享阶段，TA 生成重加密密钥，PS 对密文进行重加密并将其发送给 DO，然后 DO 上传重加密密文并

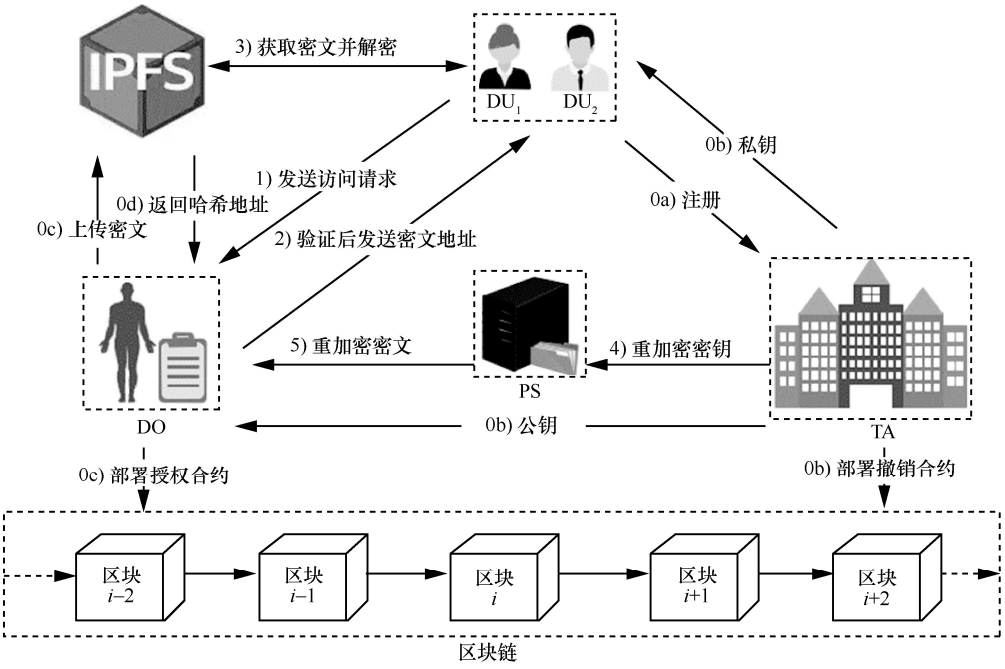


图 1　系统模型

将其相关信息存储在区块链上，后续过程与访问控制阶段相同。

3.2 安全模型

通过概率多项式时间敌手 $\mathcal{A}$ 和挑战者 $\mathcal{B}$ 之间的游戏来定义方案在选择明文攻击下的安全性，挑战者 $\mathcal{B}$ 模拟协议执行并回答来自 $\mathcal{A}$ 的查询，具体如下。

初始化 敌手 $\mathcal{A}$ 输出挑战向量 $\boldsymbol{p}_0$ 和 $\boldsymbol{p}_1$。

设置 挑战者 $\mathcal{B}$ 运行 Setup(λ) 算法生成公共参数 PP 和主密钥 MSK，将 PP 发送给 $\mathcal{A}$。

阶段 1 $\mathcal{A}$ 可以进行一系列的密钥查询，但有以下限制：$\langle \boldsymbol{p}_0, \boldsymbol{u} \rangle \neq 0$ 和 $\langle \boldsymbol{p}_1, \boldsymbol{u} \rangle \neq 0$。$\mathcal{B}$ 执行密钥生成算法 $\text{GenKey}(\text{PP}, \text{MSK}, \boldsymbol{u})$，将结果发送给 $\mathcal{A}$。

挑战 $\mathcal{A}$ 发送给挑战者两段等长的消息 M_0 和 M_1。$\mathcal{B}$ 随机选择 $w \in (0,1)$，执行加密算法 $C_w = \text{Encrypt}(\text{PP}, M_w, \boldsymbol{P}_w)$，将 C_w 发送给 $\mathcal{A}$。

阶段 2 与阶段 1 相同。

猜测 $\mathcal{A}$ 猜测 $w' \in \{0,1\}$，即 C_w 是由 M_0 还是 M_1 加密而来。定义敌手 $\mathcal{A}$ 在上述游戏中获胜的优势为

$$Adv = \left| \Pr[w' = w] - \frac{1}{2} \right|$$

定义 1 如果在任意多项式时间内，敌手只能以可忽略的优势赢得上述游戏，则称该方案在此模型中是安全的。

3.3 属性向量和策略向量生成算法

本节利用向量压缩技术提出了一种高效的属性向量和策略向量生成算法，该算法不仅可以支持正负号与门访问结构，而且通过拓展可以支持多属性值与门访问结构，具体如算法 1 所示。

算法 1 生成属性向量和策略向量

输入 给定策略集合 $P = \{P_1, P_2, \cdots, P_L\}$ 和属性集合 $U = \{U_1, U_2, \cdots, U_L\}$

输出 策略向量和属性向量

1) 策略集合中的正号负号以及通配符被分成位置集合 I、正号集合 J 和负号集合 K。

2) while $k_w \in I$ do

3) 展开 $\prod_{k_w \in I} (i - k_w) = \sum_{j=0}^{n} a_j i^j$ 得到多项式的系数 a_j

4) end while

5) for $k_w \in I$ and $i \in J$ do

6) 计算 $\prod_J = + \sum_{i \in J} \prod_{k_w \in I} (i - k_w)$

7) end for

8) for $k_w \in I$ and $i \in K$ do

9) 计算 $\prod_K = + \sum_{i \in K} \prod_{k_w \in I} (i - k_w)$

10) 计算 $\Pi = \prod_J + \prod_K$

11) end for

12) 将属性集合中的“+”“–”分成位置集合 J'和 K'

13) for i =1 to l and $i \in J'$ do

14) 计算 $\{ u_j = + \sum_{i \in J'} i^j \}$

15) end for

16) for i =1 to l and $i \in K'$ do

17) 计算 $\{ u'_j = + \sum_{i \in K'} i^j \}$

18) end for

19) 计算 $u_j = u'_j + u''_j$

20)返回策略向量和属性向量 $\boldsymbol{p} = (a_0, a_1, \cdots, a_n, 0_{n+1}, \cdots, 0_l, \Pi)$，$\boldsymbol{u} = (u_0, u_1, \cdots, u_l, -1)$

该算法是基于式(3)构建的，首先根据策略集合中通配符的位置和韦达定理构造一个 n 次多项式（n 为通配符的个数），得到多项式的系数 a_j。然后将策略集合中正负号的位置代入该多项式并求和获取 $\prod$，从而得到策略向量。最后分别对属性集合中正负号的位置进行指数运算并将对应的次数求和，从而得到属性向量。

例如，在表 1 中访问策略 $P_2 = (+, -, *, *)$，通配符位置集合 $I = \{3,4\}$，正号集合 $J = \{1\}$，负号集合 $K = \{2\}$，根据韦达定理有 $a_2 = 1, a_1 = -7, a_0 = 12$。因此可以得到策略向量元素如表 2 所示。

表 2 策略向量元素

向量元素	取值
a_0	12
a_1	−7
a_2	1
Π	(1−3)(1−4)+(2−3)(2−4)

Alice 属性 $u_{\text{Alice}} = (+, -, +, -)$，正号集合 $J' = \{1,3\}$，负号集合 $K' = \{2,4\}$，因此可以得到属性向量元素如表 3 所示。

表 3　　属性向量元素

向量元素	+	−	u_j
u_0	1^0+3^0	2^0+4^0	4
u_1	1^1+3^1	2^1+4^1	10
u_2	1^2+3^2	2^2+4^2	30

计算 $\boldsymbol{pu}=12\times4-7\times10+1\times30-8=0$

因此 Alice 满足访问策略 P_2。

3.4　智能合约设计

智能合约主要包括以下 2 个部分。

1) 撤销合约。该合约由 TA 部署，负责管理系统中已经注销的用户，主要包括以下函数。

updateAssert()。该函数负责更新撤销列表，将注销的用户放入撤销列表中。

getAssert()。该函数返回 true 或 false，用来判断用户是否被撤销。

2) 授权合约。该合约由 DO 部署，负责存储密文相关信息，当 DU 发送访问请求时调用撤销合约对其身份进行检查，从而判断是否发送密文相关信息，主要包括以下函数。

initStorage()。该函数负责存储密文相关信息。

judge()。该函数在访问控制阶段调用撤销合约中的 getAssert()函数，根据结果决定是否发送密文信息。

3.5　具体方案

本文方案主要分为 2 个阶段，即访问控制阶段和数据共享阶段。具体如下。

阶段 1　访问控制

1) Setup(λ)。该算法由 TA 执行，基于安全参数 λ，选取随机数 $(z,a_0,a_1,\cdots,a_n)\in\mathbb{Z}_p$，计算 $g_1=g^{a_1},\cdots,\ g_n=g^{a_n},\ g_0=g^z,\ h_1=h^{a_1},\cdots,h_n=h^{a_n},\ h_0=h^{a_0}$，输出 $\mathrm{MSK}=(h,h_0,h_1,\cdots,h_n),\quad \mathrm{PP}=(g,g_0,g_1,\cdots,g_n,e(g,h_0))$。

2) GenKey(PP, MSK, $\boldsymbol{u}$)。该算法仍由 TA 执行，选取随机数 $R\in\mathbb{Z}_p$，根据 PP、MSK 和属性向量 $\boldsymbol{u}$，生成密钥 $\mathrm{sk}_1=h_0\prod_{i=1}^{n}h_i^{u_iR}$ 和 $\mathrm{sk}_2=h^R$，输出密钥 $\mathrm{sk}_u=(\mathrm{sk}_1,\mathrm{sk}_2,u_i)$。

3) Encrypt(PP, $\boldsymbol{p}$, M)。该算法由 DO 执行，选取随机数 $s\in\mathbb{Z}_p$，根据 PP 和访问策略 $\boldsymbol{p}$，计算 $c_0=Me(g,h_0)^s,\ c_1=g^s,\ c_{2,i}=g_0^{p_is}g_i^s,\ 1\leqslant i\leqslant n$，输出密文 $\mathrm{CT}=(c_0,c_1,c_{2,1},\cdots,c_{2,n})$。

4) On-blockchain。该算法由 DO 执行，通过交易将密文相关信息存储在区块链上，$\mathrm{Tx}=(\mathrm{id_T},\mathrm{storeAddress},\mathrm{sign})$。其中，$\mathrm{id_T}$ 为交易的摘要，storeAddress 为密文的哈希地址，由于 IPFS 是基于内容寻址的，因此 storeAddress 也为密文完整性校验码，sign 为 DO 生成的数字签名。

5) Decrypt(sk_u, CT)。该算法由 DU 执行，首先验证 DO 的数字签名，然后根据 storeAddress 获取密文并验证密文完整性，最后根据密钥 $\mathrm{sk}_u=(\mathrm{sk}_1,\mathrm{sk}_2,u_i)$，得到如下明文

$$M=e(c_1,\mathrm{sk}_1)^{-1}e\left(\prod_{i=1}^{n}(c_{2,i})^{u_i},\mathrm{sk}_2\right)c_0$$

正确性证明如下。

$$e(c_1,\mathrm{sk}_1)^{-1}e\left(\prod_{i=1}^{n}(c_{2,i})^{u_i},\mathrm{sk}_2\right)c_0=e\left(g^s,h_0\prod_{i=1}^{n}(h_i)^{u_iR}\right)^{-1}\cdot e\left(\prod_{i=1}^{n}\left(g_0^{p_is}(g_i)^s\right)^{u_i},h^R\right)Me(g,h_0)^s=$$

$$e(g^s,h_0)^{-1}e\left(g^s,\prod_{i=1}^{n}(h^{a_i})^{u_iR}\right)^{-1}e\left(\prod_{i=1}^{n}(g_0^{sp_iu_i}),h^R\right)\cdot e\left(\prod_{i=1}^{n}(g^{a_isu_i}),h^R\right)Me(g,h_0)^s=$$

$$e(g,h_0)^{-s}e(g,h)^{-Rs\sum_{i=1}^{n}a_iu_i}e(g,h)^{zsR\sum_{i=1}^{n}p_iu_i}\cdot e(g,h)^{Rs\sum_{i=1}^{n}a_iu_i}Me(g,h_0)^s=Me(g,h)^{zsR\langle\boldsymbol{p},\boldsymbol{u}\rangle}$$

如果 $\boldsymbol{pu}=0$，则用户可以获取明文 M。证毕。

6) Revocation。该算法由 TA 执行，通过 Solidity 中的映射类型将用户地址与 true 和 false 建立对应关系，当用户未被撤销时将其地址对应的键值设置为 true，否则设置为 false。从而解决了已经注销的用户也能访问的问题，具体如下。

mapping(address=>bool)public identify;

未被撤销 identify[userAddress]=>true;

否则 identify[userAddress]=>false;

当用户进行访问时，授权合约就可以通过用户地址对应的键值来判断是否发送密文信息。

阶段 2　数据共享（注：该阶段建立在 $\mathrm{DU_1}$ 已经获取 $\mathrm{DO_1}$ 明文数据的情况下）

阶段 1 实现了策略隐藏的细粒度访问控制，但当 $\mathrm{DU_1}$ 和 $\mathrm{DU_2}$ 进行数据共享时，$\mathrm{DO_1}$ 需要根据 $\mathrm{DU_2}$ 的属性重新生成密文，这样就造成了 $\mathrm{DO_1}$ 本地计算

开销较大。为了解决这一问题，本文利用代理重加密技术对上述方案进行了拓展，使其不仅支持访问控制而且实现了数据的共享，具体如下。

1) Setup(λ) 算法。同阶段 1。

2) Re-GenKey(MSK,u_1,p_2)。TA 首先选取随机数 $d\in\mathbb{Z}_p$，计算 h^{da_0} 并运行加密算法 Encrypt(PP,p_2,h^{da_0}) 使用 p_2 加密 h^{da_0}，输出密文 C。然后选取随机数 $R'\in\mathbb{Z}_p$，生成重加密密钥 $\mathrm{rsk}_{u_1,p_2}=\{\mathrm{rsk}_1,\mathrm{rsk}_2\}$。具体过程为

$$\mathrm{rsk}_1=h_0\prod_{i=1}^{n}(h_i^{u_i}h^{\frac{da_0}{R'}})^{R'},\mathrm{rsk}_2=h^{R'}$$

3) Re-Encrypt($\mathrm{rsk}_{u_1,p_2},C,\mathrm{CT}$)。该算法由代理服务器执行。输入 $\mathrm{rsk}_{u_1,p_2},C,\mathrm{CT}$，并计算

$$C'=e(c_1,\mathrm{rsk}_1)^{-1}e\left(\prod_{i=1}^{n}(c_{2,i})^{u_i},\mathrm{rsk}_2\right)=$$

$$e(g,h)^{zsR'\langle p_1,u_1\rangle}e(g,h)^{-sa_0}e(g,h)^{-sda_0}$$

输出重加密密文 $\mathrm{CT}'=(c_0,c_1,C,C')$。

4) On-blockchain 算法。同阶段 1。

5) Re-Decrypt($\mathrm{sk}_{u_2},\mathrm{CT}'$)。$\mathrm{DU}_2$ 验证数字签名和密文完整性后使用属性密钥 sk_{u_2} 解密 C 获取 h^{da_0}，然后计算 $e(c_1,h^{da_0})C'c_0$，从而获取明文 M。

6) Revocation 算法。同阶段 1。

4 安全性分析

定理 1 基于 DBDH 假设，在访问控制阶段，对于多项式时间敌手在游戏中满足不可区分性。

证明 如果 $\mathcal{A}$ 以不可忽略的优势 ε 赢得选择明文攻击游戏，则可以构造挑战者 $\mathcal{B}$ 以不可忽略的优势 $\frac{\varepsilon}{2}$ 解决 DBDH 假设，以下为 $\mathcal{A}$ 和 $\mathcal{B}$ 的交互过程。

初始化 敌手 $\mathcal{A}$ 输出挑战向量 $\boldsymbol{p}_0$ 和 $\boldsymbol{p}_1$。

设置 $\mathcal{B}$ 选取随机数 $z',\delta,a_1',\cdots,a_n'\in\mathbb{Z}_p$，并设置 $g_1=g^{-\delta p_1}g^{a_1'},\cdots,g_n=g^{-\delta p_n}g^{a_n'},g_0=g^{z'}g^{a},Y=e(g^a,h^b)$。$a_0=ab,a_1=-\delta p_1+a_1',\cdots,a_n=-\delta p_n+a_n',\ a_0=a_0'$。

$\mathcal{B}$ 将 $\mathrm{PP}=(g,g_0,g_1,\cdots,g_n,Y)$ 发送给 $\mathcal{A}$。

在阶段 1 中，$\mathcal{A}$ 向 $\mathcal{B}$ 询问密钥。在满足 $\langle\boldsymbol{p}_0,\boldsymbol{u}\rangle\neq0$ 以及 $\langle\boldsymbol{p}_1,\boldsymbol{u}\rangle\neq0$ 的情况下 $\mathcal{B}$ 选择随机数 $R\in\mathbb{Z}_p$，并设置

$$\mathrm{sk}_1=\prod_{i=1}^{n}(h^{-\delta p_i}h^{a_i'})^{u_iR}h^{\frac{a_i'u_ia_0'}{\delta I}},\quad \mathrm{sk}_2=h^Rh^{\frac{a_0'}{\delta I}}$$

其中，$I=\langle\boldsymbol{p},\boldsymbol{u}\rangle$，$\mathrm{sk}_1,\mathrm{sk}_2$ 为合法的密钥分布。令 $R'=R+\frac{a_0'}{\delta I}$，则有

$$\prod_{i=1}^{n}(h^{-\delta p_i}h^{a_i'})^{u_iR}h^{\frac{a_i'u_ia_0'}{\delta I}}=$$

$$\prod_{i=1}^{n}h^{-\delta p_iu_iR}h^{a_0'\delta p_iu_i\frac{1}{\delta I}}h^{-a_0'\delta p_iu_i\frac{1}{\delta I}}h^{a_i'u_iR}h^{\frac{a_i'u_ia_0'}{\delta I}}=$$

$$h^{a_0'}\prod_{i=1}^{n}(h^{-\delta p_i})^{u_i\left(R+a_0'\frac{1}{\delta I}\right)}(h^{a_i'})^{u_i\left(R+a_0'\frac{1}{\delta I}\right)}=$$

$$h^{a_0'}\prod_{i=1}^{n}(h^{-\delta p_i}h^{a_i'})^{u_i\left(R+\frac{a_0'}{\delta I}\right)}=$$

$$h_0\prod_{i=1}^{n}(h_i)^{u_iR'}$$

挑战 $\mathcal{A}$ 提交两段等长的消息 M_0 和 M_1。$\mathcal{B}$ 选择 $w\in\{0,1\}$ 返回 M_w 的加密结果 $\mathrm{CT}=\left(M_wT,g^c,(g^c)^{z'p_1+a_1'},\cdots,(g^c)^{z'p_n+a_n'}\right)$。令 $z=z'+\delta,s=c$，可得 $(g^c)^{z'p_i+a_i'}=(g^c)^{z'p_i+\delta p_i-\delta p_i+a_i'}=g_0^{p_is}g_i^{s},1\leqslant i\leqslant n$。因此，$\mathrm{CT}=(c_0,c_1,c_{2,1},\cdots,c_{2,n})$。

阶段 2 与阶段 1 相同。

猜测 敌手 $\mathcal{A}$ 输出对 w 的猜测 w'，如果 $w'=w$，则 $\mathcal{B}$ 输出 1，表示 $T=e(g,h)^{abc}$；否则输出 0，表示 $T=R$。

在挑战阶段，敌手 $\mathcal{A}$ 得到的是 $(g^c)^{z'p_i+a_i'}$，不能从中推出真正的访问策略 p_i，因此保护了访问策略的隐私。

以下分析 $\mathcal{B}$ 成功解决 DBDH 假设的概率，假设 success 事件表示 $\mathcal{B}$ 成功解决 DBDH 假设，$\gamma=0$ 表示 $T=e(g,h)^{abc}$ 成立，$\gamma=1$ 表示 $T=R$ 成立。则有

$$\Pr[\mathrm{success}]=\Pr[\mathrm{success}\mid\gamma=0]\Pr[\gamma=0]+$$
$$\Pr[\mathrm{success}\mid\gamma=1]\Pr[\gamma=1]=$$
$$\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{4}=\frac{1}{2}+\frac{\varepsilon}{2}$$

其中，如果 $T=e(g,h)^{abc}$，则 $\mathcal{B}$ 完美地模拟游戏，$\mathcal{A}$ 以 $\frac{1}{2}+\varepsilon$ 的概率赢得游戏；如果 $T=R$，则 $\mathcal{B}$ 无法模拟游戏，$\mathcal{A}$ 以 $\frac{1}{2}$ 的概率赢得游戏。

因此，$\mathcal{B}$ 解决 DBDH 假设的优势为

$$\mathrm{Adv}_{\mathrm{DBDH}}=\Pr[\mathrm{success}]-\frac{1}{2}=\frac{\varepsilon}{2}$$

因为在 DBDH 假设中 ε 是不可忽略的，所以 $\mathrm{Adv}_{\mathrm{DBDH}}$ 是不可忽略的。因此如果敌手 $\mathcal{A}$ 以不可忽

略的优势攻破选择明文攻击的安全性，则挑战者 $\mathcal{B}$ 将以不可忽略的优势解决 DBDH 假设。证毕。

定理 2　基于 DBDH 假设，在数据共享阶段，对于多项式时间敌手在游戏中满足不可区分性。

证明方法同定理 1。

5　实验与评估

5.1　实验设置

本节实验的实验环境为 Windows 10 系统，CPU 的频率为 2.9 GHz，内存为 8 GB，所选取的双线性对基于椭圆曲线 $y^2=x^3+x$，椭圆曲线的阶 r 为 160 bit，素数 q 为 1 024 bit。为了实现本文方案，首先，使用基于浏览器的集成开发环境 Remix 来编辑和编译授权合约以及撤销合约。其次，使用 IPFS 存储密文，并将其哈希地址和其他密文相关信息存储在区块链上。再次，使用 Ropsten 作为测试网络，在 MetaMask 的支持下，Ropsten 可以直接在浏览器上运行一个去中心化应用程序而不需要运行完整的以太坊节点。最后，利用 JPBC 实现本文方案。

5.2　功能特性对比

本节与近几年一些技术相近的访问控制方案进行了功能特性对比，如表 4 所示，其中“√”表示具有特定功能或使用了某种技术，“×”表示不具有特定功能或未使用某种技术。

从表 4 中可以看出，本文方案和文献[13-14,16]方案都是基于素数阶双线性群构建的，然而只有本文方案支持完全策略隐藏、非对称配对运算、区块链以及数据共享。从访问结构上来看，本文方案采用的是正负号与门结构，其他方案采用的是线性秘密共享方案结构。由算法 1 可知，本文方案的效率仅与通配符数量相关，而其他方案的效率与属性数量相关，通常在实际情况下，通配符数量远远小于属性数量，因此本文方案在访问结构上有一定的优势。同样，只有本文方案和文献[14]方案实现了访问撤销的功能。因此，本文方案在功能特性上有一定的优势。

5.3　gas 消耗量评估

由于需要在区块链上部署智能合约以及执行一些必要的函数，因此必须消耗一些 gas。一般正常范围是几万～几十万 gas。一般来说，gas 的消耗主要来自代码成本 C_{code}、存储成本 C_{storge} 以及初始化成本 C_{init}。其中，代码成本与执行交易的代码的复杂度相关，存储成本主要来自数据的添加、删除等操作，初始化成本表示第一次执行某些函数时消耗的 gas。因此，gas 消耗量可以表示为

$$\text{gas} = C_{code} + C_{storage} + C_{init}$$

区块链操作 gas 消耗量如表 5 所示，从表 5 中可以看出，本文方案智能合约 gas 消耗量较小，均在合理范围之内。

表 5　区块链操作 gas 消耗量

区块链操作	gas 消耗量
部署授权合约	286 352
部署撤销合约	288 549
撤销离职用户	29 394
存储密文信息	25 984

5.4　访问控制效率评估

本节通过仿真实验将本文方案与文献[13-14,16]方案在初始化阶段、密钥生成阶段、加密阶段、解密阶段的计算开销进行对比分析，结果如图 2 所示。由算法 1 可知，本文方案的效率仅与通配符个数有关，与属性数量无关。而文献[13-14,16]方案的效率与属性数量相关。为了便于比较，本节分析了本文方案在最坏情况下的效率，即当通配符数量等于属性数量时本文方案的效率。为了保证最终结论的准确性，采取多次测量求平均值的方法。

表 4　不同访问控制方案的功能特性对比

方案	群的阶	访问结构	策略隐藏	非对称配对	访问撤销	区块链	数据共享
文献[13] 方案	素数	线性秘密共享	部分隐藏	×	×	×	×
文献[14] 方案	素数	线性秘密共享	部分隐藏	×	√	×	×
文献[16] 方案	素数	线性秘密共享	部分隐藏	×	×	×	×
本文方案	素数	正负号与门	完全隐藏	√	√	√	√

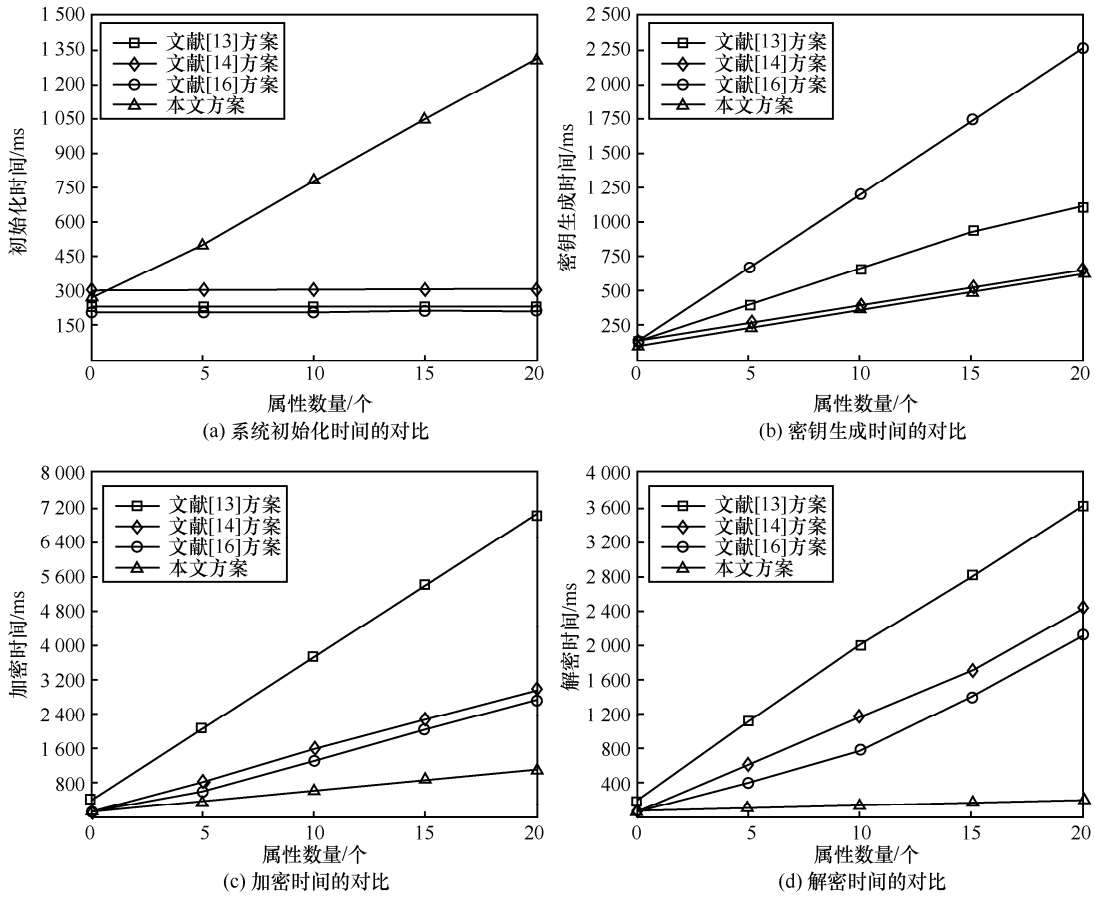


图 2　访问控制阶段计算开销对比

系统初始化时间的对比如图 2(a)所示，从图 2(a)中可以看出，本文方案的初始化时间随属性数量线性增加，而文献[13-14,16]方案所消耗的时间是基本恒定的，其中文献[16]方案所需时间最少。这是由于本文方案在设置阶段中公共参数和主密钥的大小与属性数量相关，而在文献[13-14,16]方案中是恒定不变的。

密钥生成时间的对比如图 2(b)所示，从图 2(b)中可以看出，随着属性数量的增加，本文方案与其他 3 个方案的计算开销都呈线性增加的趋势。这是由于每个存在于用户私钥中的属性都要进行相应的运算，因此属性数量越多，计算开销就越大。本文相比其他方案在密钥生成阶段计算开销相对较小，所以耗时较少。

加密时间的对比如图 2(c)所示，从图 2(c)中可以看出，本文方案和其他 3 个方案加密时间的计算开销都随着属性数量的增加而增大。其中，文献[13]方案的计算开销是最大的，本文方案由于在加密阶段中指数运算较少，因此效率较高。

解密时间的对比如图 2(d)所示，从图 2(d)中可以看出，与其他 3 个方案相比，本文方案在解密阶段的计算开销不会随属性数量的增加而发生太大的变化，并且效率明显高于其他方案。这是由于本文方案在解密阶段拥有恒定的配对次数，因此效率最高。

综上所述，本文方案虽然在初始化阶段的计算开销较大，但是在密钥生成阶段、加密阶段、解密阶段的效率均高于其他 3 个方案，因此，本文方案在性能上是最优的。

5.5　数据共享效率评估

由于文献[13-14,16]的访问控制方案不支持数据共享，为了评估本文方案的数据共享阶段的效率，本文选取了属性加密和代理加密相结合的数据共享方案[18,20]进行了对比分析，理论分析如表 6 所示，其中，E 表示描述双线性群上指数运算的时长，P 表示双线性对的运算时长，n 表示属性数量。由表 6 可知，无论是在重加密阶段还是在重解密阶段本文方案都有较高的效率。总体来说，本文方案在保证较高效率的基础上，实现了更多的功能。

表 6　数据共享阶段计算开销的理论分析

方案	重加密	重解密
文献[18]方案	$2nP$	$(n+2)E+3nP$
文献[20]方案	$nE+6P$	$2nE+6P$
本文方案	$nE+2P$	$nE+3P$

为了进一步评估数据共享阶段的效率，本节通过实验对其进行了验证，具体如图 3 所示，可以看出实验结果与理论分析一致。

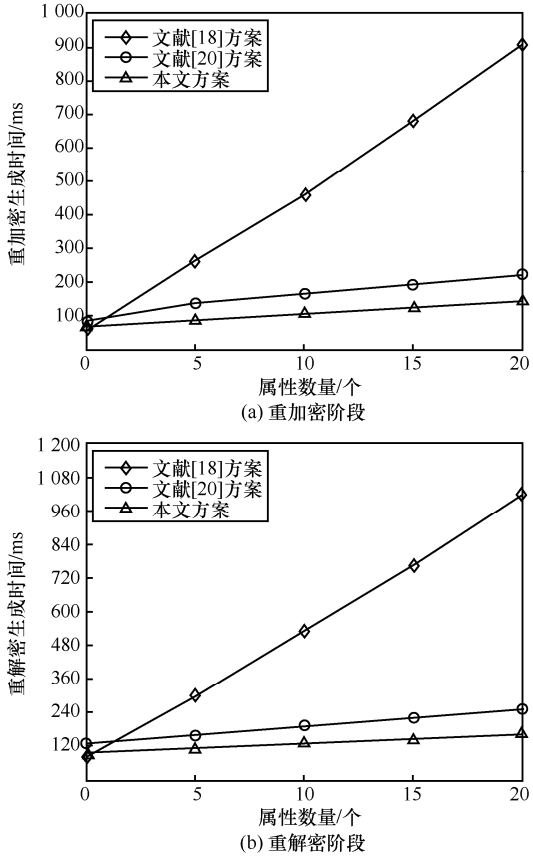


图 3　数据共享阶段计算开销的实验对比

6　结束语

本文提出了一种基于区块链且支持数据共享的密文策略隐藏访问控制方案，实现了分布式细粒度的访问控制并解决了策略隐私泄露的问题，通过使用代理重加密技术实现了支持数据共享的访问控制。此外，本文通过撤销合约维护一个撤销列表的方式实现了撤销功能，避免了用户私钥滥用问题。安全性分析和实验结果表明，本文方案是安全有效的。在未来的工作中，本文将考虑使用外包加解密技术从而降低用户的计算开销。

参考文献：

[1] BERTRAND Y, BOUDAOUD K, RIVEILL M. What do you think about your company's leaks? A survey on end-users perception toward data leakage mechanisms[J]. Frontiers in Big Data, 2020, 8: 568257.

[2] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of 2007 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2007: 321-334.

[3] BUTUN I, ÖSTERBERG P. A review of distributed access control for blockchain systems towards securing the Internet of things[J]. IEEE Access, 2021, 9: 5428-5441.

[4] XU G W, LI H W, DAI Y S, et al. Enabling efficient and geometric range query with access control over encrypted spatial data[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(4): 870-885.

[5] BOURAS M A, XIA B M, ABUASSBA A O, et al. IoT-CCAC: a blockchain-based consortium capability access control approach for IoT[J]. PeerJ Computer Science, 2021, 7: e455.

[6] SHAFEEQ S, ALAM M, KHAN A. Privacy aware decentralized access control system[J]. Future Generation Computer Systems, 2019, 101: 420-433.

[7] ZHANG Y C, LI J G, YAN H. Constant size ciphertext distributed CP-ABE scheme with privacy protection and fully hiding access structure[J]. IEEE Access, 2019, 7: 47982-47990.

[8] YU J X, HE G H, YAN X X, et al. Outsourced ciphertext-policy attribute-based encryption with partial policy hidden[C]//Information Security and Cryptology. Berlin: Springer, 2019: 448-467.

[9] SAINI A, ZHU Q Y, SINGH N, et al. A smart-contract-based access control framework for cloud smart healthcare system[J]. IEEE Internet of Things Journal, 2021, 8(7): 5914-5925.

[10] ZHANG Y Y, YUTAKA M, SASABE M, et al. Attribute-based access control for smart cities: a smart-contract-driven framework[J]. IEEE Internet of Things Journal, 2021, 8(8): 6372-6384.

[11] PHUONG T V X, YANG G M, SUSILO W. Hidden ciphertext policy attribute-based encryption under standard assumptions[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(1): 35-45.

[12] 王悦, 樊凯. 隐藏访问策略的高效 CP-ABE 方案[J]. 计算机研究与发展, 2019, 56(10): 2151-2159.
WANG Y, FAN K. Effective CP-ABE with hidden access policy[J]. Journal of Computer Research and Development, 2019, 56(10): 2151-2159.

[13] GAN T Y, LIAO Y J, LIANG Y K, et al. Partial policy hiding attribute-based encryption in vehicular fog computing[J]. Soft Computing, 2021, 25(16): 10543-10559.

[14] ZHANG W, ZHANG Z S, XIONG H, et al. PHAS-HEKR-CP-ABE: partially policy-hidden CP-ABE with highly efficient key revocation in cloud data sharing system[J]. Journal of Ambient Intelligence and

Humanized Computing, 2022, 13(1): 613-627.

[15] HAO J L, HUANG C, NI J B, et al. Fine-grained data access control with attribute-hiding policy for cloud-based IoT[J]. Computer Networks, 2019, 153: 1-10.

[16] ARKIN G, HELIL N. Ciphertext-policy attribute based encryption with selectively-hidden access policy[J]. Computing and Informatics, 2021, 40(5): 1136-1159.

[17] ZENG P, ZHANG Z T, LU R X, et al. Efficient policy-hiding and large universe attribute-based encryption with public traceability for Internet of medical things[J]. IEEE Internet of Things Journal, 2021, 8(13): 10963-10972.

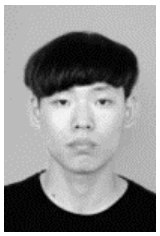
[18] GAO J T, YU H Y, ZHU X Q, et al. Blockchain-based digital rights management scheme via multiauthority ciphertext-policy attribute-based encryption and proxy re-encryption[J]. IEEE Systems Journal, 2021, 15(4): 5233-5244.

[19] 张小红, 孙岚岚. 属性代理重加密的区块链密文云存储共享研究[J]. 系统仿真学报, 2020, 32(6): 1009-1020.
ZHANG X H, SUN L L. Attribute proxy re-encryption for ciphertext storage sharing scheme on blockchain[J]. Journal of System Simulation, 2020, 32(6): 1009-1020.

[20] PAUL A, SELVI S S D, RANGAN C P. Efficient attribute-based proxy re-encryption with constant size ciphertexts[C]//Progress in Cryptology - INDOCRYPT 2020. Berlin: Springer, 2020: 644-665.

[作者简介]

杜瑞忠（1975− ），男，河北献县人，博士，河北大学教授、博士生导师，主要研究方向为可信计算、信息安全等。



张添赫（1997− ），男，河北保定人，河北大学硕士生，主要研究方向为信息安全、访问控制、区块链等。

石朋亮（1992− ），男，河北保定人，河北大学讲师，主要研究方向为分布式计算、云存储安全等。